PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-285026
(43)Date of publication of application : 13.10.2000

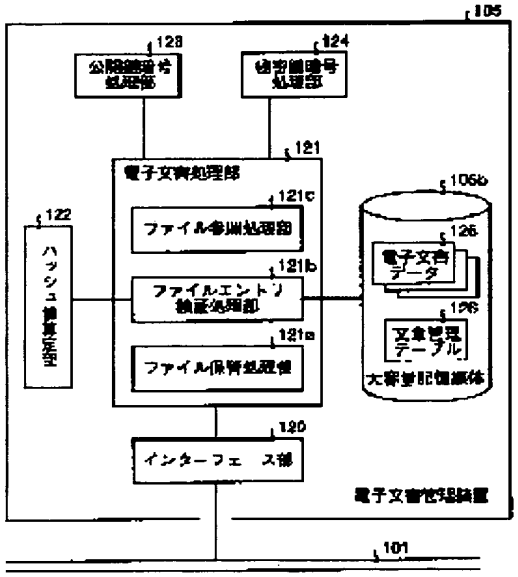
(51)Int.Cl. G06F 12/14
G06F 12/00
G09C 1/00
H04L 9/32
// G06F 17/30

(21)Application number : 11-093852
(22)Date of filing : 31.03.1999

(71)Applicant : RICOH CO LTD
(72)Inventor : KANAI YOICHI

(54) ELECTRONIC DOCUMENT MANAGEMENT SYSTEM, ITS MANAGING METHOD AND COMPUTER READABLE RECORDING MEDIUM RECORDING PROGRAM FOR EXECUTING THE METHOD BY COMPUTER

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an electronic(E) document management system capable of quickly outputting access permission to a regal user while efficiently preventing the generation of an unapproved access to an E document and the alteration of an E document, an E document managing method and a recording medium.
SOLUTION: In the case of storing an E document, a file storage processing part 121a calculates an entry signature by ciphering the hash value of a temporary file consisting of the file name of the E document, a document signature obtained by ciphering the document hash value of E document data by a private key and an access limitation list by the private key and stores a file entry to which the entry signature is added in a document management table 126 stored in a large capacity storage medium 105b.



LEGAL STATUS

[Date of request for examination] 20.06.2003
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2000－285026
（P2000－285026A）
(43)公開日　平成12年10月13日(2000.10.13)

(51)Int.Cl.[7]		識別記号	FI		テーマコード（参考）
Ｇ０６Ｆ	12/14	３２０	Ｇ０６Ｆ	12/14	３２０Ｂ　５Ｂ０１７
	12/00	５３７		12/00	５３７Ａ　５Ｂ０７５
Ｇ０９Ｃ	1/00	６４０	Ｇ０９Ｃ	1/00	６４０Ｂ　５Ｂ０８２
		６６０			６６０Ｄ　５Ｊ１０４
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７１　９Ａ００１

審査請求　未請求　請求項の数11　ＯＬ　（全 12 頁）　最終頁に続く

(21)出願番号　特願平11－93852

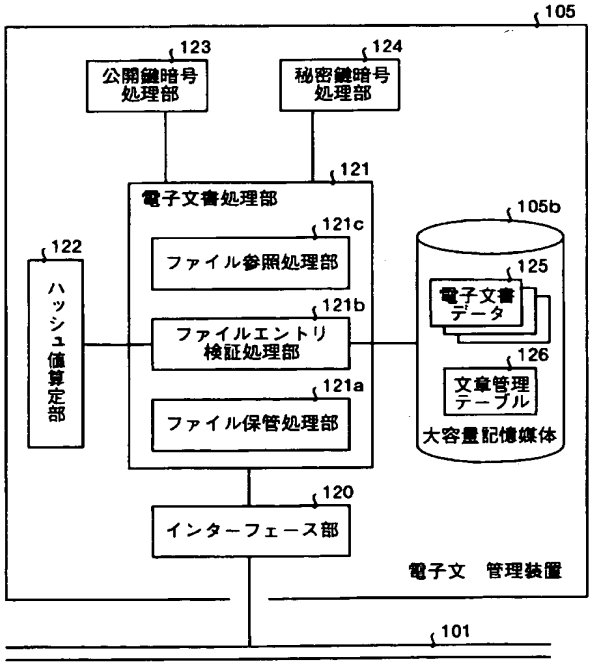
(22)出願日　平成11年３月31日(1999.3.31)

(71)出願人　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号
(72)発明者　金井　洋一
東京都大田区中馬込１丁目３番６号　株式会社リコー内
(74)代理人　100089118
弁理士　酒井　宏明

最終頁に続く

(54)【発明の名称】　電子文書管理システム、電子文書管理方法およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体

(57)【要約】
【課題】　電子文書に対する許可なきアクセスや電子文書の改ざんを効率良く防止しつつ、正当なユーザに対するアクセス許可を迅速におこなうことができる電子文書管理システム、電子文書管理方法および記録媒体を提供すること。
【解決手段】　ファイル保管処理部１２１ａが電子文書を保管する際に、電子文書のファイル名と、電子文書データの文書ハッシュ値をプライベートキーで暗号化した文書署名と、アクセス制限リストとからなる仮ファイルエントリのハッシュ値をプライベートキーで暗号化したエントリ署名を算定し、このエントリ署名を追加したファイルエントリを大容量記憶媒体１０５ｂの文書管理テーブル１２６に保管する。



1

【特許請求の範囲】

【請求項１】　電子文書を送信するクライアントと、前記クライアントから受信した電子文書を暗号化して記憶部に保管するとともに、該記憶部に保管した電子文書へのアクセスを所定のアクセス制限リストに基づいて制限する電子文書管理装置とをネットワークを介して接続した電子文書管理システムにおいて、

前記文書管理装置は、

公開鍵暗号の秘密鍵を用いて前記クライアントから受信した電子文書を暗号化して該電子文書の電子署名を取得する電子署名取得手段と、

前記電子署名取得手段が取得した電子署名および前記アクセス制限リストをその一部に含むファイルエントリを前記電子文書とともに前記記憶部に保管する保管手段と、

前記記憶部に保管した電子文書をアクセスする際に、該電子文書のファイルエントリに含まれる電子署名を前記秘密鍵に対応する公開鍵を用いて復号化して該電子文書の正当性を検証する正当性検証手段とを備えたことを特徴とする電子文書管理システム。

【請求項２】　前記保管手段は、前記電子文書に付与されたアクセス制限リストおよび前記電子署名を含むデータを前記秘密鍵を用いて暗号化してファイルエントリの正当性の有無を示すエントリ署名を取得するエントリ署名取得手段と、前記エントリ署名取得手段が取得したエントリ署名を前記ファイルエントリに追加する追加手段とを備え、前記正当性検証手段は、前記記憶部に保管した電子文書をアクセスする際に、前記エントリ署名を前記公開鍵を用いて復号化して該ファイルエントリに含まれるアクセス制限リストの改ざんを検出する改ざん検出手段を備えたことを特徴とする請求項１に記載の電子文書管理システム。

【請求項３】　前記電子文書管理装置は、前記電子文書を乱数を用いて暗号化する電子文書暗号化手段と、前記電子文書暗号化手段が用いた乱数を前記公開鍵を用いて暗号化して暗号化乱数を生成する暗号化乱数生成手段と、前記暗号化乱数生成手段が生成した暗号化乱数を前記ファイルエントリに登録するとともに、前記電子文書暗号化手段が暗号化した電子文書を前記記憶部に格納する電子文書制御手段とをさらに備え、前記正当性検証手段は、前記電子文書および前記ファイルエントリが正当であると判断された際に、該ファイルエントリに含まれる暗号化乱数を前記秘密鍵を用いて復号化して前記乱数を取得する乱数取得手段と、前記乱数取得手段が取得した乱数を用いて前記暗号化された電子文書を復号する電子文書復号手段とを備えたことを特徴とする請求項１または２に記載の電子文書管理システム。

【請求項４】　前記電子署名取得手段は、前記クライアントから受信した電子文書の文書ハッシュ値を算定する文書ハッシュ値算定手段と、前記文書ハッシュ値算定手段が算定した文書ハッシュ値を前記公開鍵暗号の秘密鍵を用いて暗号化して前記電子文書の電子署名を算定する電子署名算定手段とを備えたことを特徴とする請求項１、２または３に記載の電子文書管理システム。

2

【請求項５】　前記エントリ署名取得手段は、前記電子文書のファイル名、前記文書署名取得手段が取得した電子署名および前記アクセス制限リストからなるデータのエントリハッシュ値を算定するエントリハッシュ値算定手段と、前記エントリハッシュ値算定手段が算定したエントリハッシュ値を前記秘密鍵を用いて暗号化してファイルエントリの正当性の有無を示すエントリ署名を算定するエントリ署名算定手段とを備えたことを特徴とする請求項２、３または４に記載の電子文書管理システム。

【請求項６】　電子文書を送信するクライアントから受信した電子文書を暗号化して記憶部に保管し、該記憶部に保管した電子文書へのアクセスを所定のアクセス制限リストに基づいて制限する電子文書管理方法において、

公開鍵暗号の秘密鍵を用いて前記クライアントから受信した電子文書を暗号化して該電子文書の電子署名を取得する電子署名取得工程と、

前記電子署名取得工程で取得した電子署名および前記アクセス制限リストをその一部に含むファイルエントリを前記電子文書とともに前記記憶部に保管する保管工程と、

前記記憶部に保管した電子文書をアクセスする際に、該電子文書のファイルエントリに含まれる電子署名を前記秘密鍵に対応する公開鍵を用いて復号化して該電子文書の正当性を検証する正当性検証工程とを含んだことを特徴とする電子文書管理方法。

【請求項７】　前記保管工程は、前記電子文書に付与されたアクセス制限リストおよび前記電子署名を含むデータを前記秘密鍵を用いて暗号化してファイルエントリの正当性の有無を示すエントリ署名を取得するエントリ署名取得工程と、前記エントリ署名取得工程で取得したエントリ署名を前記ファイルエントリに追加する追加工程とを備え、前記正当性検証工程は、前記記憶部に保管した電子文書をアクセスする際に、前記エントリ署名を前記公開鍵を用いて復号化して該ファイルエントリに含まれるアクセス制限リストの改ざんを検出することを特徴とする請求項６に記載の電子文書管理方法。

【請求項８】　前記電子文書を乱数を用いて暗号化する電子文書暗号化工程と、前記電子文書暗号化工程で用いた乱数を前記公開鍵を用いて暗号化して暗号化乱数を生成する暗号化乱数生成工程と、前記暗号化乱数生成工程で生成した暗号化乱数を前記ファイルエントリに登録するとともに、前記電子文書暗号化工程で暗号化した電子文書を前記記憶部に格納する格納工程とをさらに備え、前記正当性検証工程は、前記電子文書および前記ファイルエントリが正当であると判断された際に、該ファイルエントリに含まれる暗号化乱数を前記秘密鍵を用いて復

号化して前記乱数を取得する乱数取得工程と、前記乱数取得工程で取得した乱数を用いて前記暗号化された電子文書を復号する電子文書復号工程とを含んだことを特徴とする請求項６または７に記載の電子文書管理方法。

【請求項９】　前記電子署名取得工程は、前記クライアントから受信した電子文書の文書ハッシュ値を算定する文書ハッシュ値算定工程と、前記文書ハッシュ値算定工程で算定した文書ハッシュ値を前記公開鍵暗号の秘密鍵を用いて暗号化して前記電子文書の電子署名を算定する電子署名算定工程とを含んだことを特徴とする請求項６、７または８に記載の電子文書管理方法。

【請求項１０】　前記エントリ署名取得工程は、前記電子文書のファイル名、前記文書署名取得工程で取得した電子署名および前記アクセス制限リストからなるデータのエントリハッシュ値を算定するエントリハッシュ値算定工程と、前記エントリハッシュ値算定工程で算定したエントリハッシュ値を前記秘密鍵を用いて暗号化してファイルエントリの正当性の有無を示すエントリ署名を算定するエントリ署名算定工程とを含んだことを特徴とする請求項７、８または９に記載の電子文書管理方法。

【請求項１１】　前記請求項６～１０のいずれか一つに記載された方法をコンピュータに実行させるプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、電子文書を送信するクライアントから受信した電子文書を暗号化して記憶部に保管し、該記憶部に保管した電子文書へのアクセスを所定のアクセス制限リストに基づいて制限する電子文書管理システム、電子文書管理方法および記録媒体に関し、特に、電子文書に対する許可なきアクセスや電子文書の改ざんを効率良く防止しつつ、正当なユーザに対するアクセス許可を迅速におこなうことができる電子文書管理システム、電子文書管理方法および記録媒体に関する。

【０００２】

【従来の技術】従来、電子文書を管理する電子文書管理システムでは、システム内部に蓄積した電子文書のセキュリティの確保が重要な機能の一つとして位置づけられており、かかる電子文書は、明らかに不正なユーザだけではなくシステムを管理するシステム管理者であっても原則としてアクセスできるものであってはならない。

【０００３】すなわち、蓄積した電子文書のアクセス制御をおこなう場合には、通常はシステム管理者にアクセス特権を付与することが多いが、かかるシステム管理者は、あくまでもシステム自体を管理する管理者であって、電子文書の内容を管理する者ではないので、システム管理者といえども、全ての電子文書の内容を閲覧できる特権を与えるのは妥当ではない。

【０００４】このため、特開平９－２１８８２７号公報には、認証システム名とユーザ名とアクセス権とを設定したアクセス権リストを電子文書に付与して、この電子文書をアクセス権リストとともに暗号化する電子文書管理装置が開示されている。

【０００５】

【発明が解決しようとする課題】しかしながら、かかる従来技術では、本来秘匿する必要のないアクセス権リストを電子文書とともに暗号化するために、単にアクセス権の有無を調べる場合であっても、データ量の多い電子文書全体を復号化しなければならないために効率的ではない。

【０００６】特に、カラー画像データなどが挿入された電子文書を考えると、電子文書自体のデータ量が膨大なデータ量を有するため、アクセスの許否を確認する都度電子文書を復号することとすると、処理遅延が生じるために現実的ではない。

【０００７】このため、システム管理者をも含めた不正なユーザからの電子文書に対する許可なきアクセスや電子文書の改ざんを効率良く防止しつつ、正当なユーザに対するアクセス許可を迅速におこなうことができる電子文書管理システムをいかに実現するかが極めて重要な課題となっている。

【０００８】この発明は、上記問題（課題）に鑑みてなされたものであり、システム管理者をも含めた不正なユーザからの電子文書に対する許可なきアクセスや電子文書の改ざんを効率良く防止しつつ、正当なユーザに対するアクセス許可を迅速におこなうことができる電子文書管理システム、電子文書管理方法およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体を提供することを目的とする。

【０００９】

【課題を解決するための手段】上記目的を達成するために、請求項１の発明に係る電子文書管理システムは、電子文書を送信するクライアントと、前記クライアントから受信した電子文書を暗号化して記憶部に保管するとともに、該記憶部に保管した電子文書へのアクセスを所定のアクセス制限リストに基づいて制限する電子文書管理装置とをネットワークを介して接続した電子文書管理システムにおいて、前記文書管理装置は、公開鍵暗号の秘密鍵を用いて前記クライアントから受信した電子文書を暗号化して該電子文書の電子署名を取得する電子署名取得手段と、前記電子署名取得手段が取得した電子署名および前記アクセス制限リストをその一部に含むファイルエントリを前記電子文書とともに前記記憶部に保管する保管手段と、前記記憶部に保管した電子文書をアクセスする際に、該電子文書のファイルエントリに含まれる電子署名を前記秘密鍵に対応する公開鍵を用いて復号化して該電子文書の正当性を検証する正当性検証手段とを備

えたことを特徴とする。

【００１０】この請求項１の発明によれば、公開鍵暗号の秘密鍵を用いてクライアントから受信した電子文書を暗号化して該電子文書の電子署名を取得し、取得した電子署名およびアクセス制限リストをその一部に含むファイルエントリを電子文書とともに記憶部に保管し、保管した電子文書をアクセスする際に、該電子文書のファイルエントリに含まれる電子署名を秘密鍵に対応する公開鍵を用いて復号化して該電子文書の正当性を検証することとしたので、記憶部に記憶された電子文書に対する不正な改ざんを検知することができる。

【００１１】また、請求項２の発明に係る電子文書管理システムは、前記保管手段は、前記電子文書に付与されたアクセス制限リストおよび前記電子署名を含むデータを前記秘密鍵を用いて暗号化してファイルエントリの正当性の有無を示すエントリ署名を取得するエントリ署名取得手段と、前記エントリ署名取得手段が取得したエントリ署名を前記ファイルエントリに追加する追加手段とを備え、前記正当性検証手段は、前記記憶部に保管した電子文書をアクセスする際に、前記エントリ署名を前記公開鍵を用いて復号化して該ファイルエントリに含まれるアクセス制限リストの改ざんを検出する改ざん検出手段を備えたことを特徴とする。

【００１２】この請求項２の発明によれば、電子文書に付与されたアクセス制限リストおよび電子署名を含むデータを秘密鍵を用いて暗号化してファイルエントリの正当性の有無を示すエントリ署名を取得し、取得したエントリ署名をファイルエントリに追加し、記記憶部に保管した電子文書をアクセスする際に、エントリ署名を公開鍵を用いて復号化して該ファイルエントリに含まれるアクセス制限リストの改ざんを検出することとしたので、アクセス制限リストに不正な改ざんがなされた場合であっても、その改ざんを検知して電子文書に対する不正なアクセスを防止することができる。

【００１３】また、請求項３の発明に係る電子文書管理システムは、前記電子文書管理装置は、前記電子文書を乱数を用いて暗号化する電子文書暗号化手段と、前記電子文書暗号化手段が用いた乱数を前記公開鍵を用いて暗号化して暗号化乱数を生成する暗号化乱数生成手段と、前記暗号化乱数生成手段が生成した暗号化乱数を前記ファイルエントリに登録するとともに、前記電子文書暗号化手段が暗号化した電子文書を前記記憶部に格納する電子文書制御手段とをさらに備え、前記正当性検証手段は、前記電子文書および前記ファイルエントリが正当であると判断された際に、該ファイルエントリに含まれる暗号化乱数を前記秘密鍵を用いて復号化して前記乱数を取得する乱数取得手段と、前記乱数取得手段が取得した乱数を用いて前記暗号化された電子文書を復号する電子文書復号手段とを備えたことを特徴とする。

【００１４】この請求項３の発明によれば、電子文書を

乱数を用いて暗号化し、この暗号化に用いた乱数を公開鍵を用いて暗号化して暗号化乱数を生成し、生成した暗号化乱数をファイルエントリに登録するとともに、暗号化した電子文書を記憶部に格納し、電子文書およびファイルエントリが正当であると判断された際に、該ファイルエントリに含まれる暗号化乱数を秘密鍵を用いて復号化して乱数を取得し、取得した乱数を用いて暗号化された電子文書を復号することとしたので、不正ユーザによる電子文書の入手を防止することができる。

【００１５】また、請求項４の発明に係る電子文書管理システムは、前記電子署名取得手段は、前記クライアントから受信した電子文書の文書ハッシュ値を算定する文書ハッシュ値算定手段と、前記文書ハッシュ値算定手段が算定した文書ハッシュ値を前記公開鍵暗号の秘密鍵を用いて暗号化して前記電子文書の電子署名を算定する電子署名算定手段とを備えたことを特徴とする。

【００１６】この請求項４の発明によれば、クライアントから受信した電子文書の文書ハッシュ値を算定し、算定した文書ハッシュ値を公開鍵暗号の秘密鍵を用いて暗号化して電子文書の電子署名を算定することとしたので、文書ハッシュ値という指標を用いて電子文書の不正な改ざんを効率良く検知することができる。

【００１７】また、請求項５の発明に係る電子文書管理システムは、前記エントリ署名取得手段は、前記電子文書のファイル名、前記文書署名取得手段が取得した電子署名および前記アクセス制限リストからなるデータのエントリハッシュ値を算定するエントリハッシュ値算定手段と、前記エントリハッシュ値算定手段が算定したエントリハッシュ値を前記秘密鍵を用いて暗号化してファイルエントリの正当性の有無を示すエントリ署名を算定するエントリ署名算定手段とを備えたことを特徴とする。

【００１８】この請求項５の発明によれば、電子文書のファイル名、電子署名およびアクセス制限リストからなるデータのエントリハッシュ値を算定し、算定したエントリハッシュ値を秘密鍵を用いて暗号化してファイルエントリの正当性の有無を示すエントリ署名を算定することとしたので、エントリハッシュ値という指標を用いて効率良くアクセス制限リストの改ざんを検知することができる。

【００１９】また、請求項６の発明に係る電子文書管理方法は、電子文書を送信するクライアントから受信した電子文書を暗号化して記憶部に保管し、該記憶部に保管した電子文書へのアクセスを所定のアクセス制限リストに基づいて制限する電子文書管理方法において、公開鍵暗号の秘密鍵を用いて前記クライアントから受信した電子文書を暗号化して該電子文書の電子署名を取得する電子署名取得工程と、前記電子署名取得工程で取得した電子署名および前記アクセス制限リストをその一部に含むファイルエントリを前記電子文書とともに前記記憶部に保管する保管工程と、前記記憶部に保管した電子文書を

アクセスする際に、該電子文書のファイルエントリに含まれる電子署名を前記秘密鍵に対応する公開鍵を用いて復号化して該電子文書の正当性を検証する正当性検証工程とを含んだことを特徴とする。

【００２０】この請求項６の発明によれば、公開鍵暗号の秘密鍵を用いてクライアントから受信した電子文書を暗号化して該電子文書の電子署名を取得し、取得した電子署名およびアクセス制限リストをその一部に含むファイルエントリを電子文書とともに記憶部に保管し、保管した電子文書をアクセスする際に、該電子文書のファイルエントリに含まれる電子署名を秘密鍵に対応する公開鍵を用いて復号化して該電子文書の正当性を検証することとしたので、記憶部に記憶された電子文書に対する不正な改ざんを検知することができる。

【００２１】また、請求項７の発明に係る電子文書管理方法は、前記保管工程は、前記電子文書に付与されたアクセス制限リストおよび前記電子署名を含むデータを前記秘密鍵を用いて暗号化してファイルエントリの正当性の有無を示すエントリ署名を取得するエントリ署名取得工程と、前記エントリ署名取得工程で取得したエントリ署名を前記ファイルエントリに追加する追加工程とを備え、前記正当性検証工程は、前記記憶部に保管した電子文書をアクセスする際に、前記エントリ署名を前記公開鍵を用いて復号化して該ファイルエントリに含まれるアクセス制限リストの改ざんを検出することを特徴とする。

【００２２】この請求項７の発明によれば、電子文書に付与されたアクセス制限リストおよび電子署名を含むデータを秘密鍵を用いて暗号化してファイルエントリの正当性の有無を示すエントリ署名を取得し、取得したエントリ署名をファイルエントリに追加し、記記憶部に保管した電子文書をアクセスする際に、エントリ署名を公開鍵を用いて復号化して該ファイルエントリに含まれるアクセス制限リストの改ざんを検出することとしたので、アクセス制限リストに不正な改ざんがなされた場合であっても、その改ざんを検知して電子文書に対する不正なアクセスを防止することができる。

【００２３】また、請求項８の発明に係る電子文書管理方法は、前記電子文書を乱数を用いて暗号化する電子文書暗号化工程と、前記電子文書暗号化工程で用いた乱数を前記公開鍵を用いて暗号化して暗号化乱数を生成する暗号化乱数生成工程と、前記暗号化乱数生成工程で生成した暗号化乱数を前記ファイルエントリに登録するとともに、前記電子文書暗号化工程で暗号化した電子文書を前記記憶部に格納する格納工程とをさらに備え、前記正当性検証工程は、前記電子文書および前記ファイルエントリが正当であると判断された際に、該ファイルエントリに含まれる暗号化乱数を前記秘密鍵を用いて復号化して前記乱数を取得する乱数取得工程と、前記乱数取得工程で取得した乱数を用いて前記暗号化された電子文書を復号する電子文書復号工程とを含んだことを特徴とする。

【００２４】この請求項８の発明によれば、電子文書を乱数を用いて暗号化し、この暗号化に用いた乱数を公開鍵を用いて暗号化して暗号化乱数を生成し、生成した暗号化乱数をファイルエントリに登録するとともに、暗号化した電子文書を記憶部に格納し、電子文書およびファイルエントリが正当であると判断された際に、該ファイルエントリに含まれる暗号化乱数を秘密鍵を用いて復号化して乱数を取得し、取得した乱数を用いて暗号化された電子文書を復号することとしたので、不正ユーザによる電子文書の入手を防止することができる。

【００２５】また、請求項９の発明に係る電子文書管理方法は、前記電子署名取得工程は、前記クライアントから受信した電子文書の文書ハッシュ値を算定する文書ハッシュ値算定工程と、前記文書ハッシュ値算定工程で算定した文書ハッシュ値を前記公開鍵暗号の秘密鍵を用いて暗号化して前記電子文書の電子署名を算定する電子署名算定工程とを含んだことを特徴とする。

【００２６】この請求項９の発明によれば、クライアントから受信した電子文書の文書ハッシュ値を算定し、算定した文書ハッシュ値を公開鍵暗号の秘密鍵を用いて暗号化して電子文書の電子署名を算定することとしたので、文書ハッシュ値という指標を用いて電子文書の不正な改ざんを効率良く検知することができる。

【００２７】また、請求項１０の発明に係る電子文書管理方法は、前記エントリ署名取得工程は、前記電子文書のファイル名、前記文書署名取得工程で取得した電子署名および前記アクセス制限リストからなるデータのエントリハッシュ値を算定するエントリハッシュ値算定工程と、前記エントリハッシュ値算定工程で算定したエントリハッシュ値を前記秘密鍵を用いて暗号化してファイルエントリの正当性の有無を示すエントリ署名を算定するエントリ署名算定工程とを含んだことを特徴とする。

【００２８】この請求項１０の発明によれば、電子文書のファイル名、電子署名およびアクセス制限リストからなるデータのエントリハッシュ値を算定し、算定したエントリハッシュ値を秘密鍵を用いて暗号化してファイルエントリの正当性の有無を示すエントリ署名を算定することとしたので、エントリハッシュ値という指標を用いて効率良くアクセス制限リストの改ざんを検知することができる。

【００２９】また、請求項１１の発明に係る記録媒体は、前記請求項６～１０のいずれか一つに記載された方法をコンピュータに実行させるプログラムを記録したことで、そのプログラムが機械読み取り可能となり、これによって、請求項６～１０の動作をコンピュータによって実現することができる。

【００３０】

【発明の実施の形態】以下に添付図面を参照して、この

発明に係る電子文書管理システム、電子文書管理方法およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体の好適な実施の形態を詳細に説明する。

【００３１】図２は、本実施の形態に係る電子文書管理システムの全体構成と電子文書管理装置のハードウエア構成とを示す図である。同図（ａ）に示すように、この電子文書管理システムは、クライアント１０２～１０４と、電子文書管理装置１０５とが、ネットワーク１０１に接続されたシステム構成となる。

【００３２】クライアント１０２～１０４は、電子文書１１０を作成する文書処理機能と、作成した電子文書１００の電子文書管理装置１０５への保管依頼機能と、電子文書管理装置１０５に保管した電子文書の参照および編集機能とを有する。

【００３３】電子文書管理装置１０５は、クライアント１０２～１０４から保管依頼を受けた電子文書１００を内部の大容量記憶媒体に保管する機能と、クライアント１０２～１０４の要求に応じて該当する電子文書１００をクライアントに送信する機能とを有する。

【００３４】ここで、この電子文書管理装置１０５は、クライアント１０２～１０４から受け付けた電子文書１００の保管および取り出しを単におこなうのではなく、電子文書１００自体の不正な改ざんや、電子文書１００に対するアクセス制限を記述したアクセス制限リストの不正な改ざんを電子署名（ディジタル署名）を用いて検出できるよう構成している。

【００３５】また、この電子文書管理装置１０５では、電子文書１００を平文で記憶するだけではなく、この電子文書１００を暗号化して記憶することもできる。なお、かかる暗号化処理をおこなった場合には、正当なクライアントのみが電子文書１００の正しい暗号鍵を入手できることとしている。

【００３６】図２（ｂ）に示すように、この電子文書管理装置１０５は、プロセッサ１０５ａと、プログラム格納媒体１０５ｂと、大容量記憶媒体１０５ｃと、通信ポート１０５ｄとからなる。

【００３７】プロセッサ１０５ａは、プログラム格納媒体１０５ｂに格納した各種のプログラムを読み込んで、電子文書に係る各種処理を実行する処理部であり、プログラム格納媒体１０５ｂは、文書管理プログラム、ハッシュプログラム、暗号化プログラムおよび復号化プログラムなどの各種プログラムを記憶する記憶部である。

【００３８】ここで、この文書管理プログラムは、暗号化プログラムおよび復号化プログラムの処理に必要となる公開鍵暗号系のプライベートキーを内在し、かかるプライベートキーは、外部からは読み出すことはできないものとする。

【００３９】また、ここで言う暗号化プログラムおよび復号化プログラムには、電子文書を暗号化および復号化するためのＤＥＳ（Data Encryption Standard）暗号と、このＤＥＳ暗号で用いる鍵や後述するハッシュ値を暗号化または復号化するための公開鍵暗号の両者が含まれる。

【００４０】大容量記憶媒体１０５ｃは、ハードディスクドライブ（ＨＤＤ）、ＣＤ－ＲまたはＭＯなどの書き換え可能な記録媒体からなる電子文書などを記憶する記憶部であり、通信ポート１０５ｄは、この電子文書装置１０５をネットワーク１０１に接続するための接続端子である。なお、ここでは説明の便宜上、この大容量記憶媒体１０５ｃをプログラム格納媒体１０５ｂと別個に設けた場合を示したが、両者を同じ記録媒体上に設けることもできる。

【００４１】次に、本実施の形態に係る電子文書管理装置１０５の具体的な構成について説明する。図１は、本実施の形態に係る電子文書管理装置１０５の構成を示す機能ブロック図である。同図に示すように、この電子文書管理装置１０５は、インターフェース部１２０と、電子文書処理部１２１と、ハッシュ値算定部１２２と、公開鍵暗号処理部１２３と、秘密鍵暗号処理部１２４と、大容量記憶媒体１０５ｂとからなる。

【００４２】インターフェース部１２０は、図２（ｂ）に示す通信ポート１０５ｄおよびネットワーク１０１を介してクライアント１０２～１０４との間でデータ授受をおこなうネットワークインターフェースである。

【００４３】電子文書処理部１２１は、クライアント１０２～１０４からネットワーク１０１を介して受け取った電子文書の保管や、クライアント１０２～１０４の要求に応答して電子文書の送信などをおこなう本装置の主体をなす処理部であり、ファイル保管処理部１２１ａと、ファイルエントリ検証処理部１２１ｂと、ファイル参照処理部１２１ｃとを有する。

【００４４】ここで、このファイル保管処理部１２１ａは、クライアント１０２～１０４から受け取った電子文書を保管する処理部であり、具体的には、クライアント１０２～１０４から電子文書とともにこの電子文書を暗号化する旨を示すフラグを受け取ったならば、この電子文書を乱数で暗号化した電子文書データを作成し、暗号化しない旨のフラグを受け取った場合には、乱数をによる電子文書の暗号化はおこなわない。

【００４５】また、このファイル保管処理部１２１ａは、単に電子文書データを保管するだけではなく、保管する電子文書のファイルエントリを作成し、作成したファイルエントリを文書管理テーブル１２６に追加する処理をおこなう。

【００４６】ここで、このファイルエントリは、電子文書のファイル名と、電子文書のハッシュ値をプライベートキーで暗号化した文書署名と、アクセス制限リストと、これらで形成される仮ファイルエントリのハッシュ値をプライベートキーで暗号化したエントリ署名と、電

子文書の暗号化に用いた乱数をパブリックキーで暗号化した暗号化乱数とからなる。

【００４７】また、ファイルエントリ検証処理部１２１ｂは、ファイル保管処理部１２１ａが文書管理テーブル１２６に追加したファイルエントリの検証をおこなう処理部である。さらに、ファイル参照処理部１２１ｃは、クライアント１０２～１０４の要求に応答して大容量記憶媒体１０５ｂに記憶した電子文書ファイルを参照する処理部である。

【００４８】ハッシュ値算定部１２２は、電子文書処理部１２１の要求に応じて電子文書に対応するハッシュ値若しくは電子文書のファイル名、文書署名およびアクセス制限リストで形成される仮ファイルエントリに対応するハッシュ値を算定する処理部である。

【００４９】公開鍵暗号処理部１２３は、電子文書自体を暗号化するためではなく、ハッシュ値に電子署名を施したり、電子文書の暗号化に用いた暗号鍵（乱数）を暗号化または復号化するために用いる暗号処理部である。なお、この公開鍵暗号処理部１２３では、ＲＳＡ（Rivest-Shamir-Adleman ）暗号などを用いることになる。

【００５０】秘密鍵暗号処理部１２４は、電子文書自体を暗号鍵（乱数）を用いて暗号化する際に用いる暗号処理部であり、たとえば米国商務省標準局が公布したＤＥＳ暗号（Data Encryption Standard）などを用いることができる。

【００５１】次に、図１に示すファイル保管処理部１２１ａによる電子文書の保管処理手順について具体的に説明する。図３は、このファイル保管処理部１２１ａによる電子文書の保管処理の概念を示す概念図であり、図４は、このファイル保管処理部１２１ａによる電子文書の保管処理手順を示すフローチャートである。なお、ここでは、電子文書のファイル名が「sample01.doc」であり、ファイルアクセス制限リストが、「user1　RW 、user2　R、user3　R」である場合を示している。

【００５２】図３に示すように、電子文書管理装置１０５がクライアント１０２～１０４から電子文書データ、電子文書のファイル名、アクセス制限リストおよび暗号化フラグを受け取ると、ファイル保管処理部１２１ａは、電子文書データの文書ハッシュ値を算定した後（ステップＳ４０１）、この文書ハッシュ値をプライベートキーで暗号化して文書署名を取得する（ステップＳ４０２）。

【００５３】その後、電子文書のファイル名「sample01.doc」、文書署名およびファイルアクセス制限リスト「user1　RW 、user2　R、user3　R」からなる仮ファイルエントリを作成し（ステップＳ４０３）、仮ファイルエントリのエントリハッシュ値を算定し（ステップＳ４０４）、算定したエントリハッシュ値をプライベートキーで暗号化してエントリ署名を取得し（ステップＳ４０５）、取得したエントリ署名を仮ファイルエントリに追加してファイルエントリを作成する（ステップＳ４０６）。

【００５４】ここで、暗号化フラグにより暗号化が指定されている場合には（ステップＳ４０７肯定）、秘密鍵暗号処理用の乱数を発生して電子文書データを暗号化するとともに（ステップＳ４０８）、この暗号化に用いた乱数をパブリックキーで暗号化して暗号化乱数を取得して（ステップＳ４０９）、取得した暗号化乱数をファイルエントリに追加する（ステップＳ４１０）。なお、暗号化フラグにより暗号化が指定されていない場合には（ステップＳ４０７否定）、上記ステップＳ４０８～Ｓ４１０の処理はおこなわない。

【００５５】その後、このファイルエントリを文書管理テーブル１２６に追加した後（ステップＳ４１１）、この文書管理テーブル１２６と必要に応じて暗号化した電子文書データを大容量記憶媒体１０５ｂに記録した後（ステップＳ４１２～Ｓ４１３）、作成したファイルエントリをクライアントに返して処理を終了する（ステップＳ４１４）。

【００５６】上記一連の処理をおこなうことにより、電子文書データを大容量記録媒体１０５ｂに保存する際に、暗号化されていないアクセス容易なアクセス制限リストと、電子文書の文書署名と、エントリ署名と、暗号化乱数とからなるファイルエントリを文書管理テーブル１２６に登録することができる。

【００５７】なお、上記ファイルエントリをクライアントを返すこととしたのは、クライアントの指示に応答して電子文書が正しく保管されたか否かをパブリックキーを利用して検証できるようにするためである。

【００５８】そこで、次に図１に示すファイルエントリ検証処理部１２１ｂによる処理手順について説明する。図５は、図１に示すファイルエントリ検証処理部１２１ｂの処理手順を示すフローチャートである。同図に示すように、このファイルエントリ検証処理部１２１ｂは、クライアントからファイルエントリの検証指示を受け付けたならば、このファイルエントリからエントリ署名を取得するとともに（ステップＳ５０１）、ファイル名、文書署名およびアクセス制御リストを取得する（ステップＳ５０２）。

【００５９】そして、これらのデータから仮ファイルエントリを作成し（ステップＳ５０３）、作成した仮ファイルエントリのエントリハッシュ値を取得する（ステップＳ５０４）。また、ファイルエントリから取得したエントリ署名をパブリックキーで復号して検証ハッシュ値とし（ステップＳ５０５）、この検証ハッシュ値とエントリハッシュ値とを比較する（ステップＳ５０６）。

【００６０】その結果、両者が一致する場合には（ステップＳ５０７肯定）、電子文書が正常に保管されたものと判定してその旨をクライアントに返送し（ステップＳ５０８）、両者が一致しない場合には（ステップＳ５０

７否定）、電子文書が正常に保管されなかったものと判定してその旨をクライアントに返送する（ステップＳ５０９）。上記一連の処理をおこなうことにより、クライアントの要求に応じて電子文書が正常に保管されたか否かをパブリックキーに基づいて確認することができる。

【００６１】次に、図１に示すファイル参照処理部１２１ｃによるファイル参照手順について説明する。図６は、図１に示すファイル参照処理部１２１ｃによるファイル参照手順を示すフローチャートである。同図に示すように、このファイル参照処理部１２１ｃは、大容量記憶媒体１０５ｂから文書管理テーブル１２６を読み出し（ステップＳ６０１）、読み出した文書管理テーブル１２６から該当する電子文書のファイルエントリを取得し（ステップＳ６０２）、このファイルエントリからアクセス制御リストを取得する（ステップＳ６０３）。

【００６２】そして、図５を用いて説明したファイルエントリの検証処理を実行し（ステップＳ６０４）、ファイルエントリが正当なものであるか否かを確認する（ステップＳ６０５）。この場合には、図５のステップＳ５０８はファイルエントリが正当な場合に対応し、ステップＳ５０９はファイルエントリが正当でない場合に対応する。

【００６３】そして、このファイルエントリが正当でないと判定された場合には（ステップＳ６０５否定）、エラー処理をおこない（ステップＳ６１０）、ファイルエントリが正当であると判定された場合には（ステップＳ６０５肯定）、ファイルエントリに暗号化乱数があるか否かを確認し（ステップＳ６０６）、暗号化乱数がある場合には（ステップＳ６０６肯定）、この暗号化乱数をプライベートキーで復号して乱数を取得し（ステップＳ６０７）、取得した乱数で電子文書ファイルを復号して電子文書データを取得し（ステップＳ６０８）、取得した電子文書データをクライアントに返送する（ステップＳ６０９）。これに対して、ファイルエントリに暗号化乱数がなければ（ステップＳ６０６否定）、そのまま電子文書データをクライアントに返送する（ステップＳ６０９）。

【００６４】上記一連の処理をおこなうことにより、大容量記憶媒体１０５ｂに記憶した電子文書データ１２５や文書管理テーブル１２６のアクセス制御リストが改ざんされた場合に、その改ざんを検出することができる。

【００６５】上述してきたように、本実施の形態では、ファイル保管処理部１２１ａが電子文書を保管する際に、電子文書のファイル名と、電子文書データの文書ハッシュ値をプライベートキーで暗号化した文書署名と、アクセス制限リストとからなる仮ファイルエントリのハッシュ値をプライベートキーで暗号化したエントリ署名を算定し、このエントリ署名を追加したファイルエントリを大容量記憶媒体１０５ｂの文書管理テーブル１２６に保管するよう構成したので、電子文書データ１２５やアクセス制限リストの改ざんを検知することができる。

【００６６】また、暗号化を示す暗号フラグが指定された際に、秘密鍵暗号処理部１２４を用いて電子文書データを乱数で暗号化して電子文書データ１２５として保管するとともに、この乱数をパブリックキーで暗号化した暗号化乱数をファイルエントリに追加するよう構成したので、正当なクライアント以外が適正に復号化した電子文書データを取得することを防止することができる。

【００６７】

【発明の効果】以上説明したように、請求項１の発明によれば、公開鍵暗号の秘密鍵を用いてクライアントから受信した電子文書を暗号化して該電子文書の電子署名を取得し、取得した電子署名およびアクセス制限リストをその一部に含むファイルエントリを電子文書とともに記憶部に保管し、保管した電子文書をアクセスする際に、該電子文書のファイルエントリに含まれる電子署名を秘密鍵に対応する公開鍵を用いて復号化して該電子文書の正当性を検証するよう構成したので、記憶部に記憶された電子文書に対する不正な改ざんを検知することができる電子文書管理システムが得られるという効果を奏する。

【００６８】また、請求項２の発明によれば、電子文書に付与されたアクセス制限リストおよび電子署名を含むデータを秘密鍵を用いて暗号化してファイルエントリの正当性の有無を示すエントリ署名を取得し、取得したエントリ署名をファイルエントリに追加し、記記憶部に保管した電子文書をアクセスする際に、エントリ署名を公開鍵を用いて復号化して該ファイルエントリに含まれるアクセス制限リストの改ざんを検出するよう構成したので、アクセス制限リストに不正な改ざんがなされた場合であっても、その改ざんを検知して電子文書に対する不正なアクセスを防止することができる電子文書管理システムが得られるという効果を奏する。

【００６９】また、請求項３の発明によれば、電子文書を乱数を用いて暗号化し、この暗号化に用いた乱数を公開鍵を用いて暗号化して暗号化乱数を生成し、生成した暗号化乱数をファイルエントリに登録するとともに、暗号化した電子文書を記憶部に格納し、電子文書およびファイルエントリが正当であると判断された際に、該ファイルエントリに含まれる暗号化乱数を秘密鍵を用いて復号化して乱数を取得し、取得した乱数を用いて暗号化された電子文書を復号するよう構成したので、不正ユーザによる電子文書の入手を防止することができる電子文書管理システムが得られるという効果を奏する。

【００７０】また、請求項４の発明によれば、クライアントから受信した電子文書の文書ハッシュ値を算定し、算定した文書ハッシュ値を公開鍵暗号の秘密鍵を用いて暗号化して電子文書の電子署名を算定するよう構成したので、文書ハッシュ値という指標を用いて電子文書の不正な改ざんを効率良く検知することができる電子文書管

理システムが得られるという効果を奏する。

【００７１】また、請求項５の発明によれば、電子文書のファイル名、電子署名およびアクセス制限リストからなるデータのエントリハッシュ値を算定し、算定したエントリハッシュ値を秘密鍵を用いて暗号化してファイルエントリの正当性の有無を示すエントリ署名を算定するよう構成したので、エントリハッシュ値という指標を用いて効率良くアクセス制限リストの改ざんを検知することができる電子文書管理システムが得られるという効果を奏する。

【００７２】また、請求項６の発明によれば、公開鍵暗号の秘密鍵を用いてクライアントから受信した電子文書を暗号化して該電子文書の電子署名を取得し、取得した電子署名およびアクセス制限リストをその一部に含むファイルエントリを電子文書とともに記憶部に保管し、保管した電子文書をアクセスする際に、該電子文書のファイルエントリに含まれる電子署名を秘密鍵に対応する公開鍵を用いて復号化して該電子文書の正当性を検証するよう構成したので、記憶部に記憶された電子文書に対する不正な改ざんを検知することができる電子文書管理方法が得られるという効果を奏する。

【００７３】また、請求項７の発明によれば、電子文書に付与されたアクセス制限リストおよび電子署名を含むデータを秘密鍵を用いて暗号化してファイルエントリの正当性の有無を示すエントリ署名を取得し、取得したエントリ署名をファイルエントリに追加し、記記憶部に保管した電子文書をアクセスする際に、エントリ署名を公開鍵を用いて復号化して該ファイルエントリに含まれるアクセス制限リストの改ざんを検出するよう構成したので、アクセス制限リストに不正な改ざんがなされた場合であっても、その改ざんを検知して電子文書に対する不正なアクセスを防止することができる電子文書管理方法が得られるという効果を奏する。

【００７４】また、請求項８の発明によれば、電子文書を乱数を用いて暗号化し、この暗号化に用いた乱数を公開鍵を用いて暗号化して暗号化乱数を生成し、生成した暗号化乱数をファイルエントリに登録するとともに、暗号化した電子文書を記憶部に格納し、電子文書およびファイルエントリが正当であると判断された際に、該ファイルエントリに含まれる暗号化乱数を秘密鍵を用いて復号化して乱数を取得し、取得した乱数を用いて暗号化された電子文書を復号するよう構成したので、不正ユーザによる電子文書の入手を防止することができる電子文書管理方法が得られるという効果を奏する。

【００７５】また、請求項９の発明によれば、クライアントから受信した電子文書の文書ハッシュ値を算定し、算定した文書ハッシュ値を公開鍵暗号の秘密鍵を用いて暗号化して電子文書の電子署名を算定するよう構成したので、文書ハッシュ値という指標を用いて電子文書の不正な改ざんを効率良く検知することができる電子文書管

理方法が得られるという効果を奏する。

【００７６】また、請求項１０の発明によれば、電子文書のファイル名、電子署名およびアクセス制限リストからなるデータのエントリハッシュ値を算定し、算定したエントリハッシュ値を秘密鍵を用いて暗号化してファイルエントリの正当性の有無を示すエントリ署名を算定するよう構成したので、エントリハッシュ値という指標を用いて効率良くアクセス制限リストの改ざんを検知することができる電子文書管理方法が得られるという効果を奏する。

【００７７】また、請求項１１の発明に係る記録媒体は、前記請求項６～１０のいずれか一つに記載された方法をコンピュータに実行させるプログラムを記録したことで、そのプログラムが機械読み取り可能となり、これによって、請求項６～１０の動作をコンピュータによって実現することができる。

【図面の簡単な説明】

【図１】この実施の形態に係る電子文書管理装置の構成を示す機能ブロック図である。

【図２】本実施の形態に係る電子文書管理システムの全体構成と電子文書管理装置のハードウエア構成とを示す図である。

【図３】図１に示すファイル保管処理部による電子文書の保管処理の概念を示す概念図である。

【図４】図１に示すファイル保管処理部による電子文書の保管処理手順を示すフローチャートである。

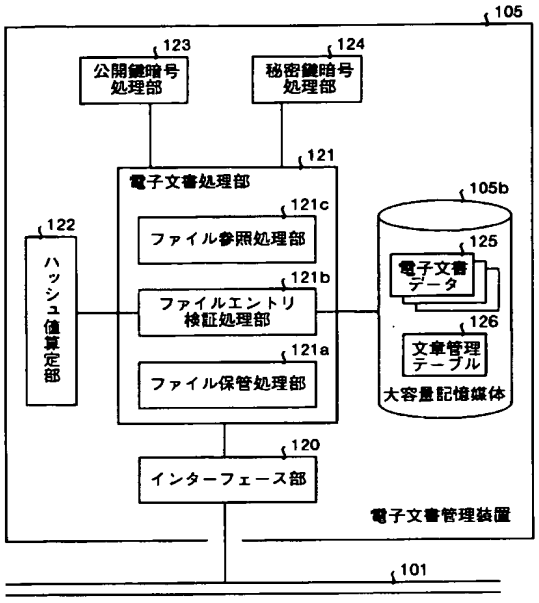
【図５】図１に示すファイルエントリ検証処理部の処理手順を示すフローチャートである。

【図６】図１に示すファイル参照処理部によるファイル参照手順を示すフローチャートである。

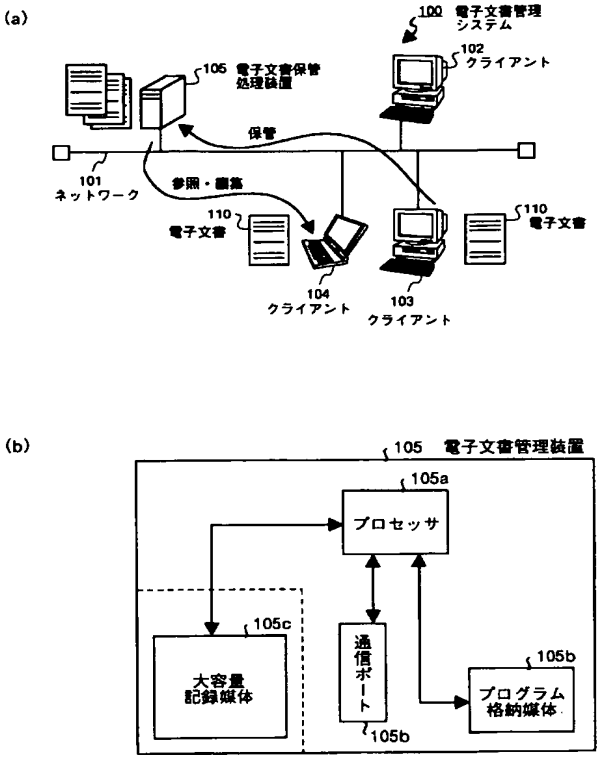
【符号の説明】

１００　電子文書管理システム
１０１　ネットワーク
１０２，１０３，１０４　クライアント
１０５　電子文書管理装置
１０５ａ　プロセッサ
１０５ｂ　プログラム格納媒体
１０５ｃ　大容量記憶媒体
１０５ｄ　通信ポート
１２０　インターフェース部
１２１　電子文書処理部
１２１ａ　ファイル保管処理部
１２１ｂ　ファイルエントリ検証処理部
１２１ｃ　ファイル参照処理部
１２２　ハッシュ値算定部
１２３　公開鍵暗号処理部
１２４　秘密鍵暗号処理部
１２５　電子文書データ
１２６　文書管理テーブル

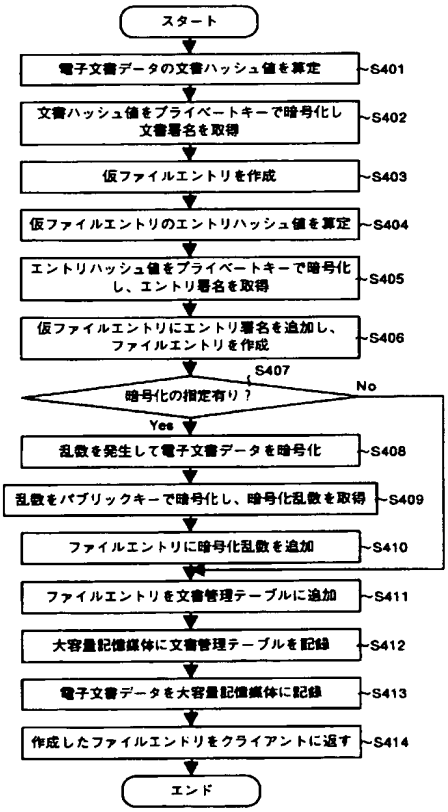
【図１】



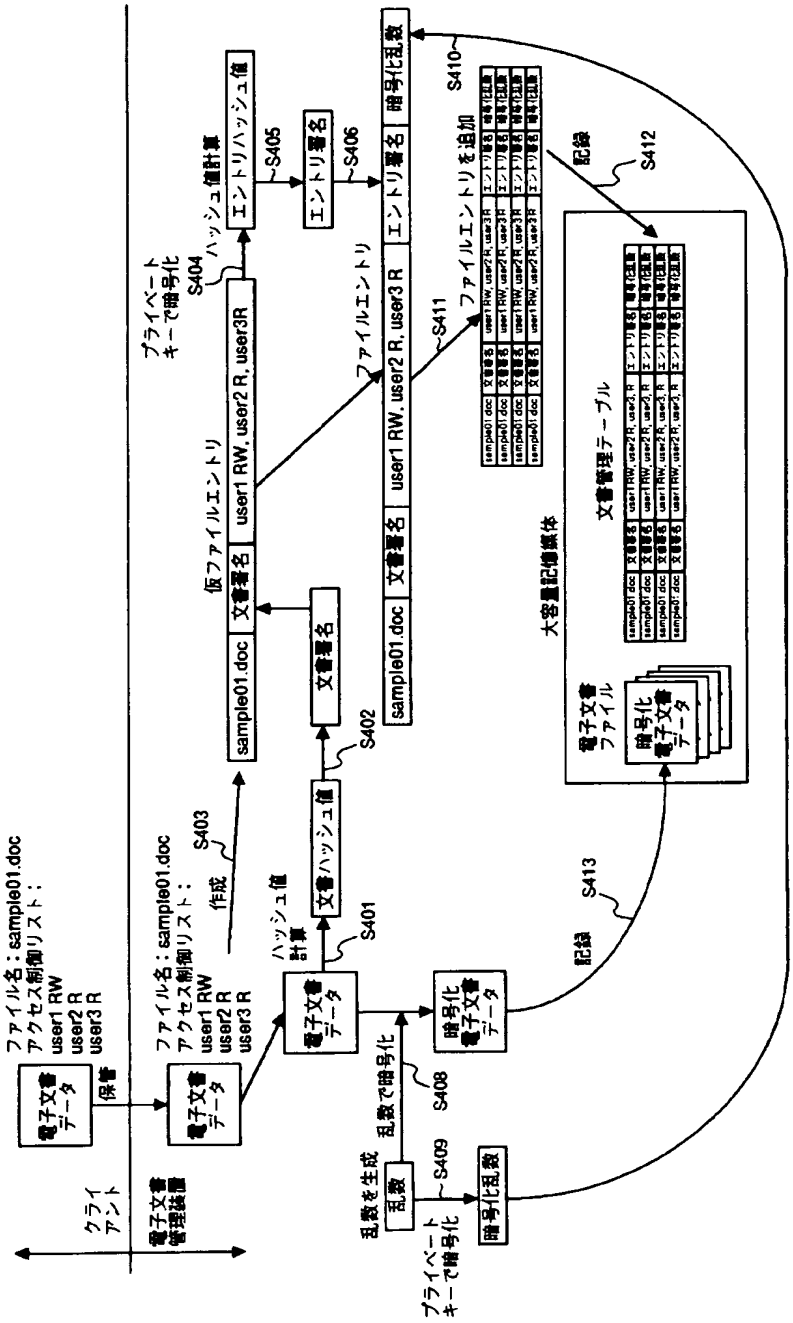
【図２】



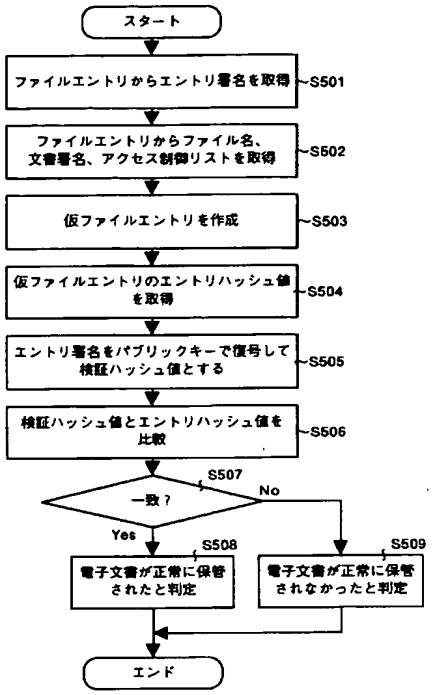
【図４】



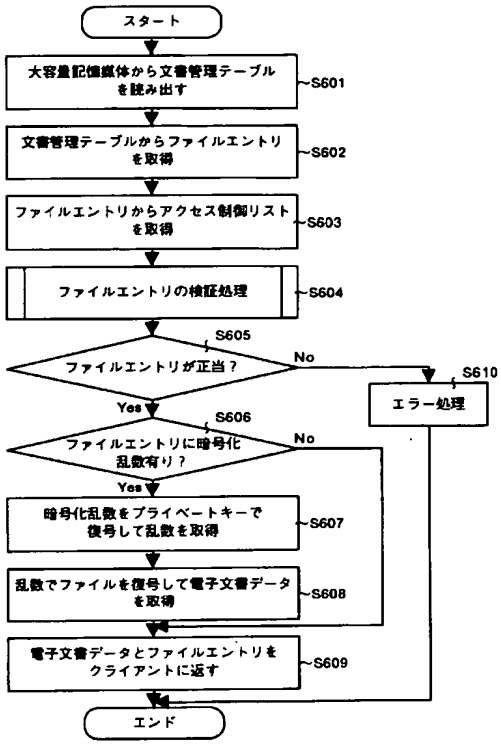
【図３】


クライアント
電子文書管理装置
ファイル名：sample01.doc
アクセス制御リスト：
user1 RW
user2 R
user3 R
電子文書データ
保管
S401
ハッシュ値計算
文書ハッシュ値
S402
文書署名
S403
作成
仮ファイルエントリ
sample01.doc
文書署名
user1 RW, user2 R, user3R
プライベートキーで暗号化
S404
ハッシュ値計算
エントリハッシュ値
S405
エントリ署名
S406
ファイルエントリ
sample01.doc
文書署名
user1 RW, user2 R, user3 R
エントリ署名
暗号化乱数
S410
S411
ファイルエントリを追加
文書管理テーブル
大容量記憶媒体
電子文書ファイル
暗号化電子文書データ
S412
記録
S413
乱数を生成
乱数
S408
乱数で暗号化
暗号化電子文書データ
S409
プライベートキーで暗号化
暗号化乱数

【図５】



【図６】



フロントページの続き

(51)Int.Cl.[7]	識別記号	F I		テーマコード(参考)
// Ｇ０６Ｆ　17/30		Ｈ０４Ｌ　9/00	６７５Ｂ	
		Ｇ０６Ｆ　15/40	３２０Ｂ	

Ｆターム(参考)　5B017 AA01 BA07 BB02 CA07 CA09
CA16
5B075 KK43 KK54 KK60 KK63 NK45
UU05
5B082 AA11 EA11 GA02 HA08
5J104 AA09 LA01 LA03 NA06 NA12
NA38 PA07 PA14
9A001 BB03 BB04 CC02 EE02 EE03
EE04 FF03 GG22 JJ13 LL03